ABSTRACT

A WIRELESS METHOD FOR MONITORING MEDICATION COMPLIANCE

by
Jeffrey Scott Jonas

There are many devices on the market to help remind patients to take their pills, but most require observation by a caregiver to assure medication compliance. This project demonstrates three modes to detect pill removal from a pillbox: a switch under the pills, a reflective type photointerrupter and a transmissive "electric eye" photosensor. Each mode exhibited blind spots or other failures to detect pill presence, but by combining modes with complementary characteristics, the accuracy of pill detection is greatly increased.

Two methods of caregiver notification are demonstrated: text messages transmitted via an attached cellular phone, or the status is collected by a PC which provides an audit trail and daily notification if no pills were taken.

A WIRELESS METHOD FOR MONITORING MEDICATION COMPLIANCE

by
Jeffrey Scott Jonas

A Thesis
Submitted to the Faculty of
New Jersey Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Engineering

Department of Electrical and Computer Engineering

August 2006

APPROVAL PAGE

A WIRELESS METHOD FOR MONITORING MEDICATION COMPLIANCE

Jeffrey Scott Jonas

Dr. Constantine M. Manikopoulos, Thesis Advisor — Date
Associate Professor of Electrical and Computer Engineering, NJIT

Dr. Quentin Jones, Committee Member — Date
Assistant Professor of Information Systems, NJIT

Dr. Swades De, Committee Member — Date
Assistant Professor of Electrical and Computer Engineering, NJIT

BIOGRAPHICAL SKETCH

Author: Jeffrey Scott Jonas

Degree: Master of Science

Date: August 2006

Undergraduate and Graduate Education:

- Master of Science in Computer Engineering,
  New Jersey Institute of Technology, Newark, NJ, 2006

- Bachelor of Science in Electrical Engineering,
  The Cooper Union, New York, NY, 1984

Major: Computer Engineering

Two roads diverged in a yellow wood,
And sorry I could not travel both
And be one traveler, long I stood
And looked down one as far as I could
To where it bent in the undergrowth;

Then took the other, as just as fair,
And having perhaps the better claim,
Because it was grassy and wanted wear;
Though as for that the passing there
Had worn them really about the same,

And both that morning equally lay
In leaves no step had trodden black.
Oh, I kept the first for another day!
Yet knowing how way leads on to way,
I doubted if I should ever come back.

I shall be telling this with a sigh
Somewhere ages and ages hence:
Two roads diverged in a wood, and I —
I took the one less traveled by,
And that has made all the difference.

-- Robert Frost

To my parents for their unconditional love and support.

ACKNOWLEDGMENT

I humbly and gratefully acknowledge all those who formed the foundation of knowledge and wisdom upon which my education has been built, especially:

My thesis advisor Dr. Constantine N. Manikopoulos and the thesis committee members for sharing their expertise in practical applications of cryptography and wireless applications.

Dr. Quentin Jones' Pervasive Computing course was the first college class I had taken in nearly 20 years. It was so challenging, stimulating and full of human interest that I enthusiastically matriculated for the NJIT master's program.

Gene Buterbaugh and Robert Lopes for sharing their knowledge of embedded systems and sensors.

Carmen Street and the staff of the N.J. Unemployment Office for the tuition waiver program that enabled me to return to college

The people of the Cooper Union School of Engineering whose confidence, faith and support led to the completion of my bachelor's degree.

- Professor Richard G. Costello for enthusiasm, humor, practical engineering and belief in my abilities.
- Robert P. Hopkins and Dean Hollander for their limitless kindness and support.
- Professors Paul Hess and Don Kunz for absolute dedication to their crafts.

The dedicated teachers and staff of Francis Lewis High School, particularly

- Theodore Liebersfeld, Howard Sardis, Howard Levine, Gerald Elgarten and Melvin Serisky for sharing their love of mathematics and computing machinery balanced with humility and a sense of community via the Math-Science Institute and International Baccalaureate program. The foundations of computer programming and analysis they established have been reaffirmed time and time again in my career and studies.
- William S. Dobkin, The Chairman of Social Studies, for recognizing and fostering my talents outside of math and science and making me a more balanced person. I am still trying to live up to his yearbook inscription "I'm a firm believer than when some great breakthrough in a momentous human endeavor will be made, you will be part of it".
- Dr. Harris Nierman for being so strict about conducting a research paper "use original sources in the original language when possible!" My appreciation and support of the NY research libraries started with his humanities research topics.

Lillian Koeppel, my 2nd grade teacher, for caring and sharing above and beyond the call of duty and channeling my curiosity into more creative endeavors.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

LIST OF TABLES

LIST OF FIGURES

DEFINITIONS

802.11	IEEE standards for WiFi (long range high speed wireless networks)
802.15	IEEE standards for PAN (Personal Area Networks: short range, low to medium speed)
AES	Advanced Encryption Standard
Auto ID	A research consortium fostering machine-readable ID technologies such as RFID. http://www.autoidlabs.org/ http://autoid.mit.edu/cs/
Bluetooth	IEEE 802.15.1 for medium speed wireless PAN
DES	Data Encryption Standard, deprecated and replaced by AES
HIPAA	the Health Insurance Portability & Accountability Act of 1996: specifies privacy requirements for all those handling patient data
HL7	Health Level Seven is an ANSI (American National Standards Institute) data exchange standard for healthcare clinical and administrative data. http://www.hl7.org/ http://en.wikipedia.org/wiki/HL7
MEMS	Micro Electro-Mechanical Systems, primarily micro sensors fabricated as part of an integrated circuit
MOTE	A miniature wireless sensor, soon to be grain-of-rice sized, or smaller
PAN	Any of the IEEE 802.15 short range Personal Area Networks
RFID	Radio Frequency Identification
WiFi	Any of the IEEE 802.11 Wide Area Wireless Network protocols
ZigBee	IEEE 802.15.4 standard for low speed wireless PAN, intended for sensor networks

CHAPTER 1

INTRODUCTON

1.1 Overview of Medication Compliance

Did you take your pill today? There are numerous pill containers trying to make it easier to track one's medicine intake: some have a container per day, others up to four containers a day. Some have timers, alarms and clocks and even auto-dispense the pills, but they all require direct observation to tell if the pills were taken at all, let alone taken at the correct time.

Figure 1.1 Pill dispensers.

Medication Compliance (diligently taking one's medicine as prescribed) is a major concern because it is a leading cause of preventable emergency room visits and avoidable illnesses.

Table 1.1 Medication Error Facts, Figures and Examples

• In 1993, a total of 7391 people died due to medication errors in the United States alone
• The cost of medication errors is estimated to be over $7 billion per year in the United States
• The annual cost of hospital-based medication related errors is estimated to be $2 billion in the United States
• In 1993, over a ten year period, outpatient deaths due to medication errors increased by 8.48-fold in the United States as opposed to a 2.37-fold increase in inpatient deaths.
• In 1986, a review of seven studies, conducted in the United States, revealed that 5.5% of hospital admissions, i.e. 1.94 million admissions, can be attributed to drug therapy noncompliance. Their total cost to hospitals was estimated to be around $8.5 billion.

Source: B. Dhillon, *Human Reliability and Error in Medical Systems*, World Scientific Publishing Company, 2003, pp. 2, 90.

1.2 Motivation

Most remote patient monitoring systems focus on chronically ill patients who require immense attention and diligence. This research proposes a low cost system for anyone who needs minimal assistance with their medication.

Many exciting technologies are flourishing at this time, particularly MEMS (Micro Electro-Mechanical Systems), embedded processing, wireless communications and sensor networks. When applied to the medical field, this means that more can be observed, measured and learned about the human body using minimally intrusive devices. It is now feasible to use a small implanted sensor for weeks, months or years monitoring many vital signs. As new sensor technology develops, it will be possible to continuously and simultaneously monitor hundreds of bodily functions at low cost.

Measuring and recording body functions are already used for athletic training, but currently require large non-portable equipment. As continuous monitoring becomes miniaturized, then medication can also evolve to a closed control loop. Instead of taking a pill every day regardless of the body's need, it will soon be possible to administer the medication by an embedded processor based on real-time sensor data of the body's current state.

For example, most diabetic patients inject themselves with insulin once a day (or more as required), but they measure their blood glucose levels to determine the required dosage. That's a closed loop system for the effect of the insulin is measured by the resulting blood glucose level and the patient adjusts the subsequent dosages accordingly. Insulin pumps [1] are small devices that administer small doses throughout the day. The simpler units deliver timed doses regardless of activity, requiring on the user to adjust dose levels if desired. New units [2] now continuously measure the blood glucose level and react accordingly without patient intervention. Such units are still rare, but demonstrate how technology is already assisting medication compliance via automatic delivery. The eventual goal is to create an artificial pancreas.

Until all medicine can be automatically machine administered, the patient is responsible for self-administering the prescription.

Most current medication compliance dispensers are too simplistic (pre fill a container a day) or too expensive, or way too ambitious and intrusive. This thesis explores ways to assist anyone who takes medicine by monitoring if any medication was taken within the usual time and informing someone to help them. Other solutions barely address this problem space.

1.3 Objective

The scope of this project is to focus on modes of detecting pills taken from the container and the wireless infrastructure required to support such monitoring. The infrastructure is a large problem space because of the availability of many competing technologies, the sudden ubiquity of wireless devices such as cellular phones, the need for privacy, security and data access control particularly when participating in monitored systems. The user interface is out of this project's scope because it is already well addressed by previous research, and because there is no need for a user interface in the minimal configurations. Ideally, the medicine tracking device will be as easy to use as a baby-monitor: buy one at any store and just turn it on.

This investigation further explores modular expansion to incorporate new technologies. One such expansion allows participation in health monitoring systems with HIPAA compliance to assure the patient's privacy while giving the freedom to live at home with minimally intrusive observation. This is unique from other prototypes for it empowers the patient to control their initial and recurring costs with a variety of configurations.

This system may be expanded to record events and make them available as needed. Avoiding expensive monitoring is preferred when feasible, although that may be useful to integrate medical compliance into the patient's medical history. For example: tracking total dosages and most recent dosages would be available to the physician or EMT. That way instead of just seeing a Medic Alert tag noting that the patient is diabetic, they can ascertain when the most recent insulin dose was administered and the dosage. Open source, community based services are advocated because they are cost

effective, independently verifiable and allow greater participation and control of personal information.

Many ambitious home monitoring systems have been proposed because there are so many variables. If too many pills are missing from the container, does it mean an accidental overdose has occurred, or just that the container has spilled, or some medication was moved to another container? Without direct observation or input from the patient, wrong guesses are inevitable despite the best of intentions and myriad of sensors.

The intention of the system is to keep people in the loop so the patient is never a "slave to the machine" but always treated with respect and dignity.

CHAPTER 2

PRIOR RESEARCH

2.1 Ubicomp

Ubicomp (Ubiquitous or Pervasive computing) is no longer science fiction. Microcontrollers, embedded systems, system-on-chip, commodity wireless systems (cellular phones, WAN, PAN) all give the building blocks for Sensor Networks in the home.

> Pervasive computing is the trend towards increasingly ubiquitous (another name for the movement is ubiquitous computing), connected computing devices in the environment, a trend being brought about by a convergence of advanced electronic - and particularly, wireless - technologies and the Internet. Pervasive computing devices are not personal computers as we tend to think of them, but very tiny - even invisible - devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods - all communicating through increasingly interconnected networks.
>
> Among the emerging technologies expected to prevail in the pervasive computing environment of the future are wearable computers, smart homes and smart buildings. Pervasive computing researchers aim to understand how to create systems that are pervasively and unobtrusively embedded in the environment, completely connected, intuitive, effortlessly portable, and constantly available, that are of social value
>
> Source: Q. Jones, "Pervasive Computing CIS686 course description," 2006, http://modiin.njit.edu/courses.html.

Much recent research focuses on applying Ubicomp principles to medication monitoring such as a "Magic medicine Cabinet" [3], [4] that automatically tracks all the medication inside of it (via RFID tags), to smaller scale sensors such as an RFID reader and scale to sense what medicine containers are placed on it and measure how much has been taken [5]

The "Smart Badge" [6] system was an early prototype that tracked people within an appropriately equipped building to facilitate helpful services such as finding co-workers and for phone calls to follow them to the nearest phone (this was before personal cellular/wireless phones were affordable and small enough to carry all the time). Several at-home monitoring systems propose using similar systems to infer the patient's activities and any changes in health. Hospitals already use RFID bracelets to accurately track patients' locations and match patients to their medications and treatments, thus increasing acceptance of such individual tracking. As biosensors are added (blood pressure, pulse, breathing rate, temperature, etc.) them the monitoring will more accurately report significant changes in health status. Eventually sufficient information will be continuously gathered to practice closed-loop control systems for medication: administering the medication solely based on the body's needs and reactions. Advanced pacemakers work autonomously but allow remote diagnostics [7], not to eliminate doctor visits but to give timely information between visits.

By definition, most RFID devices are short range, but "Project Lifesaver" [8], [9] provides watch-sized transmitters to individuals with Alzheimer's disease, autism or other debilitating disorders, and the corresponding tracking equipment to the Sheriff's Search and Rescue Unit to quickly locate a participant when reported missing or lost. The tracking range is up to several miles. Perhaps a GPS equipped cellular phone can supplement such tracking.

Even more ambitious home health systems seek to combine "smart homes" with telemedicine in order to better react to the patient's needs and for more accurate inferences of the patient's activity. Placing sensors in slippers and shoes reports if

they're getting exercise, giving timely information while avoiding personal RFID tags when possible (such as living alone). Such monitoring will semi-automate required eldercare reports such as ADL (activities of daily living) and actually increases privacy with the "invisible man" model (like in the movies, the invisible man is inferred by the objects he touches, moves and manipulates) [10], [11]. This illustration shows how medicine monitoring is just one part of the system.

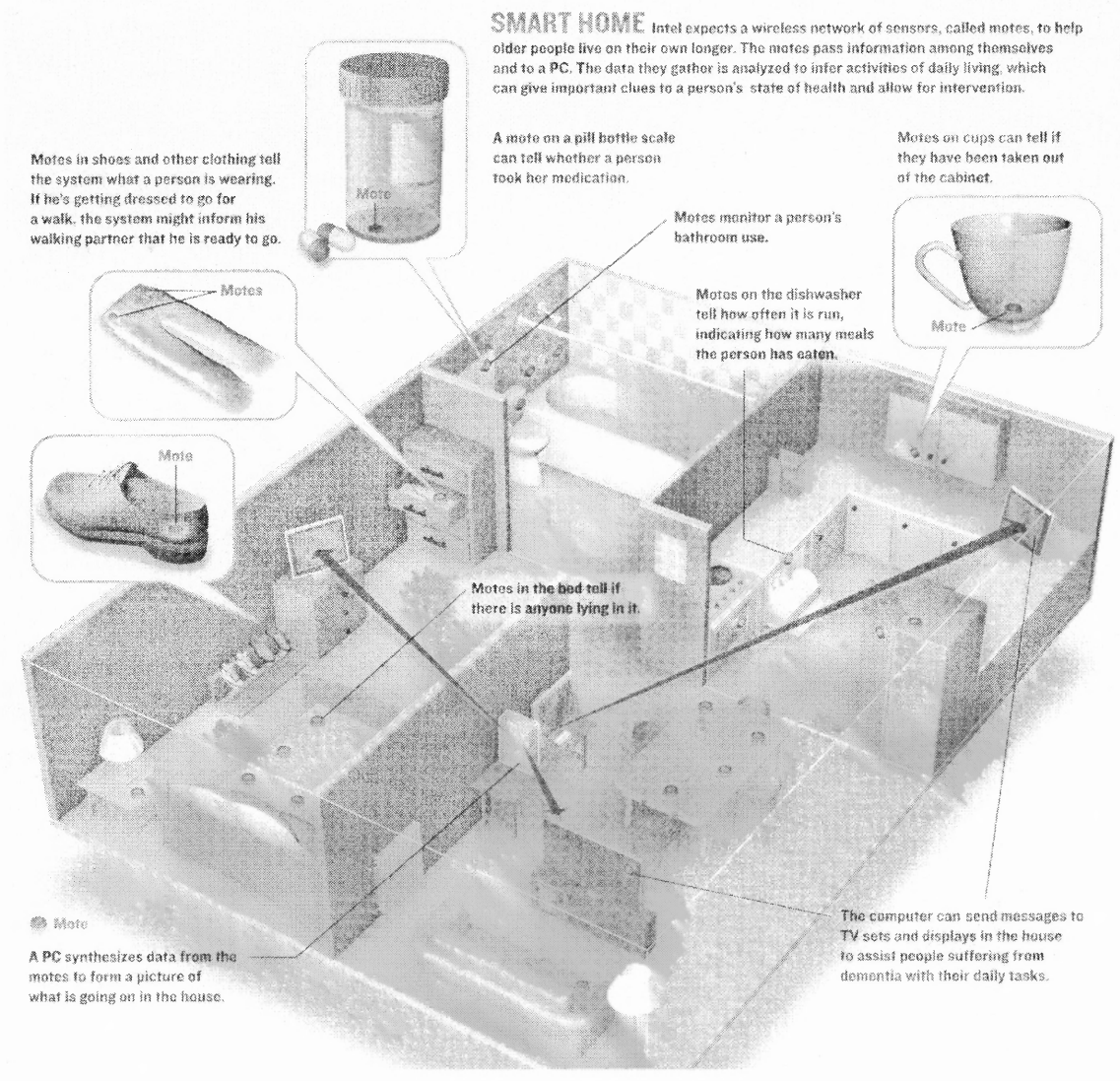


Figure 2.1 The Smart Home.
Source: P. Ross, "Managing Care Through The Air," *IEEE Spectrum*, vol 41, number 12, pp. 26-31, December 2004.

There are many dystopian visions of a future where technology alienates and dehumanizes people, such as the movies Metropolis, Modern Times, Minority Report and Gattaca. Engineering has always been a human endeavor and most professional societies (such as the IEEE, ACM, Order of the Engineer) have rules of ethics to protect society from technological abuse. This relates to the topic because privacy and ethics must be part of the design and implementation from the start, not retrofitted or left for later. It is an obligation of the engineer.

2.2 Telemedicine

The Citizen Health System is a proposed monitoring system using wireless monitoring

> Health delivery practices are shifting towards home care. The reasons are the better possibilities for managing chronic care, controlling health delivery costs, increasing quality of life and quality of health services and the distinct possibility of predicting and thus avoiding serious complications. For the above goals to become routine, new telemedicine and information technology (IT) solutions need to be implemented and integrated in the health delivery scene, and these solutions need to be assessed through evidence-based medicine in order to provide solid proof for their usefulness. Thus, the concept of contact or call centers has emerged as a new and viable reality in the field of IT for health and telemedicine. In this paper we describe a generic contact center that was designed in the context of an EU funded IST for health project with acronym Citizen Health System (CHS). Since the generic contact center is composed by a number of modules, we shall concentrate in the modules dealing with the communication between the patient and the contact center using mobile telecommunications solutions, which can act as link between the internet and the classical computer telephony communication means. We further elaborate on the development tools of such solutions, the interface problems we face, and on the means to convey information from and to the patient in an efficient and medically acceptable way. This application proves the usefulness of wireless technology in providing health care services all around the clock and everywhere the citizen is located, it proves the necessity for restructuring the medical knowledge for education delivery to the patient, and it shows the virtue of interactivity by means of using the limited, yet useful browsing capabilities of the wireless application protocol

Source: N. Maglaveras, V. Koutkias, I. Chouvarda, D. Goulis, A. Avramides, D. Adamidis, G. Louri das, EA. Balas, "Home care delivery through the mobile telecommunications platform: the Citizen Health System (CHS) perspective," *International Journal of Medical Informatics*, Volume 68, Issue 3, pp. 99-111, Dec 18 2002.

Wireless monitoring of medication is one of the many inputs upon which such systems will depend.

2.3 Other Medication Dispensers and Tracking

The most extensive home medicine dispenser [12] is about the size of a coffee-maker, holds 60 pre-filled cups, reminds the patient with voice alarm when to take medication and automatically calls a caregiver if medication is not taken. An unmonitored model is the size of a dinner plate with an inner carousel that dispenses pre-filled pills. Other variations include multi-compartment containers with reminders such as timers, alarms and clearly marked lids.

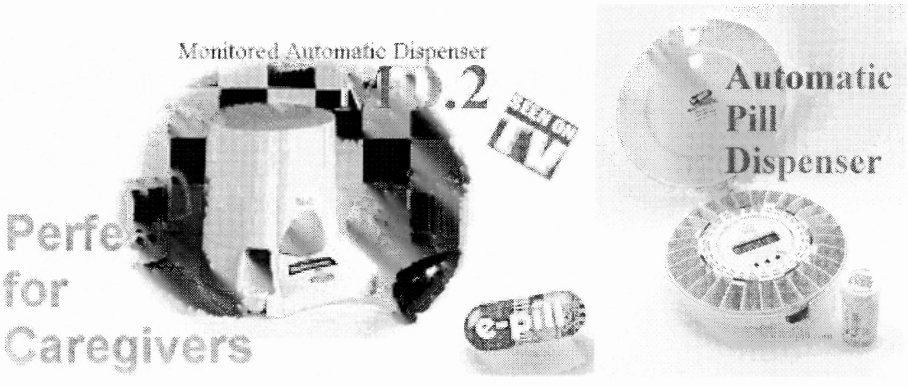


Figure 2.2 Commercial automatic pill dispenser.
Source: e-pill Medication Reminders, "Monitored Automatic Pill Dispenser MD.2 with Voice Alarm," http://www.epill.com/md2.html.

The SensorVial from Secure Packaging Systems, Inc. is a programmable RFID cap with embedded sensors for temperature and integrity that fits existing containers, enabling RFID tracking of medications.

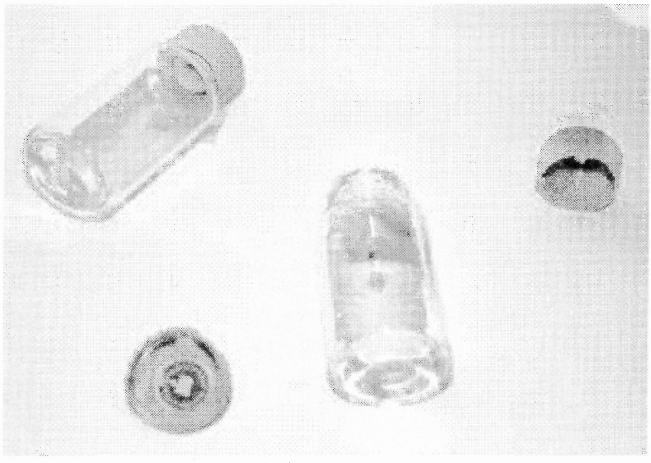
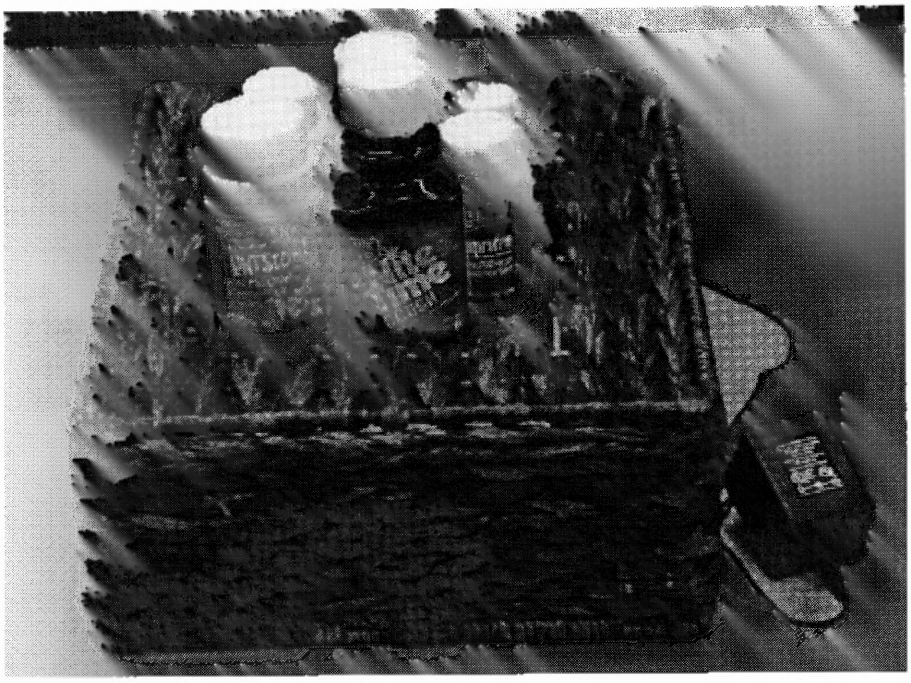


Figure 2.3 SensorVial caps.
Source: Sensorvial web site, http://www.sensorvial.com/product.html.

Intel Research Seattle [13], [14] has explored several aspects of medication compliance such as a simplified "smart shelf" by combining a scale and RFID reader so the amount of medication taken from the containers can be ascertained by their reduction in weight. RFID tags were placed on the bottoms of the medicine containers to correlate the objects being weighed with the current and previous weight. Electronic scales (such as those used by jewelers) are sensitive enough to sense individual pills.



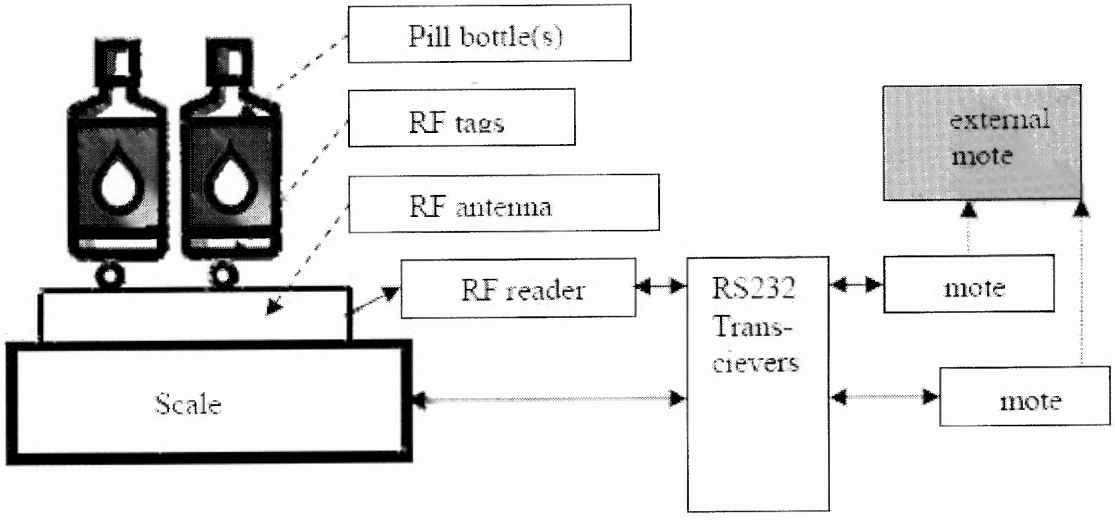


Figure 2.4 Medicine monitoring pad.
Source: K. Fiskhin, M. Wang, "A Flexible, Low-Overhead Ubiquitous System for Medication Monitoring," October 2003, http://seattleweb.intel-research.net/people/fishkin/pubs_files/medpad_tr.pdf.

CHAPTER 3

INTRODUCTION TO RFID

3.1 RFID Basics

RFID (Radio Frequency identification) tags are wireless transponders that transmit a pre-programmed ID [15] thus identifying items even if they're inside other containers (unlike barcodes that must be seen) so they're immensely popular for inventory systems and payment systems.

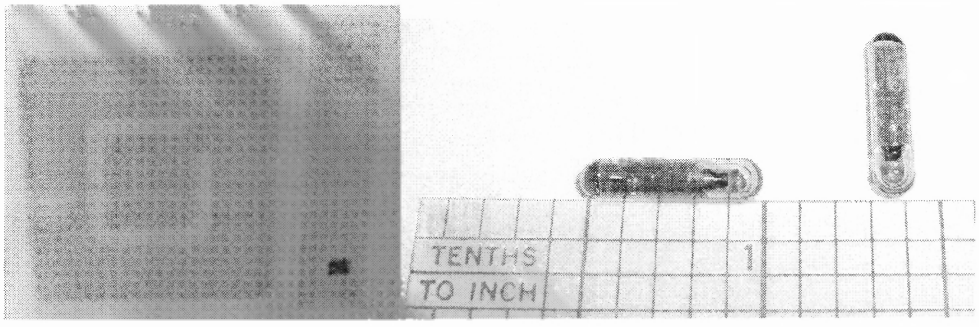


Figure 3.1 RFID tags.

Simple versions such as EAS (Electronic Article Surveillance "anti-theft tags") transmit their presence ("I am here!") to the readers by the store door even when concealed. RFID and other wireless/contactless systems (such as contactless credit cards, EZ pass and other transit payment systems) are being deployed rapidly because they offer significant advantages over existing systems such as reading many items simultaneously even if moving rapidly (trains, motor vehicles), reading items at a distance, reduced reader maintenance, and thwarting duplication or cloning of the tags

3.2 Pharmaceutical Applications

The pharmaceutical industry will soon be deploying RFID not just for tracking inventory but to thwart the infiltration of counterfeit drugs and enable precise audit trails for all products. The benefits can extend to the consumer when "smart labels" are used for the medicine dispensed to the patient. Unlike current labels that are only human-readable printed information, smart labels may contain significantly more data such as

- The medicine's pedigree: manufacturing facility, batch, formulation, expiration
- The doctor's name, ID, and link to the prescription
- The pharmacist's name, location, date it was dispensed
- The patient's name and ID

Unlike barcodes, the information can be entirely self-contained in the RFID tag, requiring no external database to decode the information. This will be of great value to caretakers, emergency medical technicians and doctors to match the patient to the medication and to research the patient's complete medication history. Electronic signatures and other safeguards prevent data tampering or counterfeiting.

Several electronic pedigree legislations in the USA are scheduled to take effect in 2007, mandating stronger accounting for drug sources, primarily to prevent counterfeiting. Some pharmaceutical manufacturers have already initiated their own incentives to protect their supply chain. RFID is the favored technology for achieving these goals, but requires vigilance at all distribution points since counterfeit drugs are often inserted deep in the supply chain, often with forged credentials.

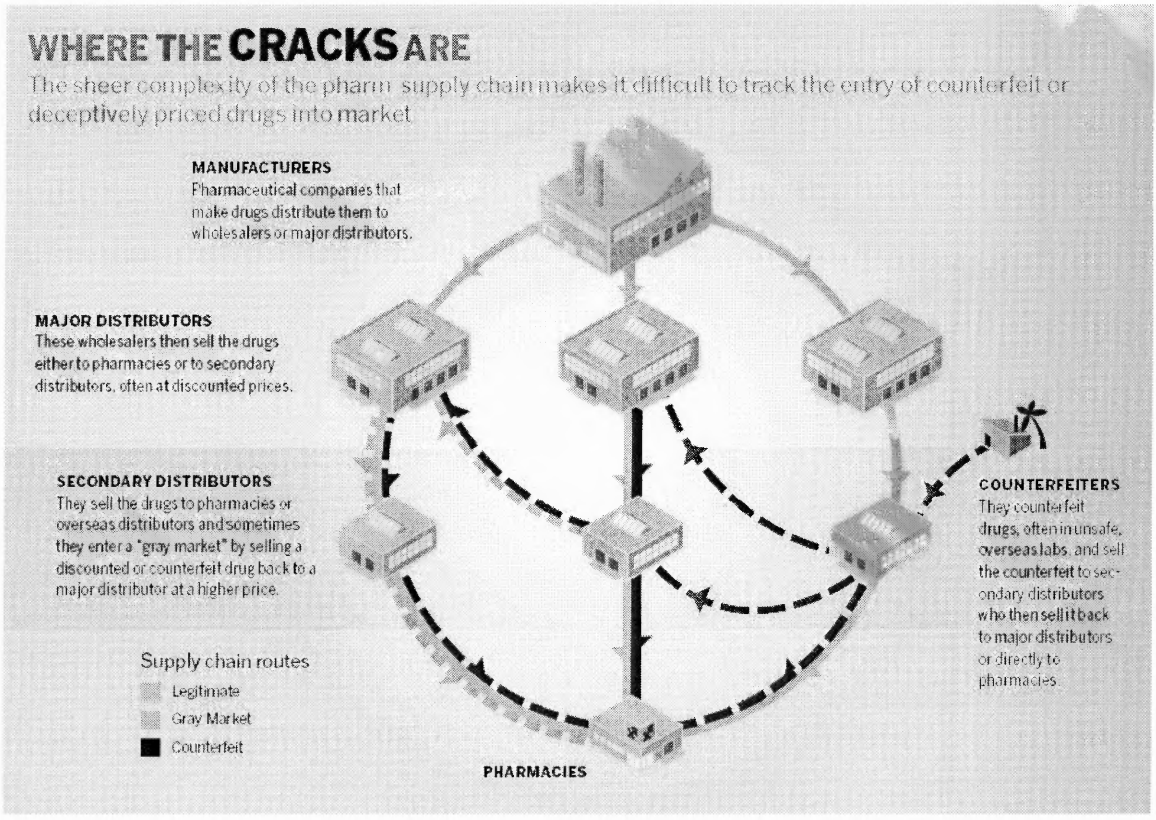


Figure 3.2 Pharmaceutical counterfeiting.
Source: S. Patton, "Cracks in the Pharmaceutical Supply Chain," *CIO Magazine*, Jan 5, 2006, http://www.cio.com/archive/011506/pharma.html.

3.3 RFID Privacy

Privacy and security are related but separate issues. Privacy is *what* you keep secret and from whom, security is *how* you do it. Privacy is a form of confidentiality; an agreement or definition of how information is shared responsibly. Military information is shared on a "need to know basis". HIPPA are legal guidelines for managing access to health records. Security provides tools to manage the secrets, such as ways to lock the information from casual access, and provides authentication ("I am Jeff" "prove it") to enforce the access policies.

Privacy is a major concern with RFID [16] because there is no off switch or activity indicator. The ambiguity of precisely what constitutes consent to access the tag has led to a battle of RFID access measures and counter-measures.

RFID access control may be achieved by various methods: temporary or permanent deactivation; temporary, permanent or conditional blocking using passive or active devices. EAS (anti-theft) tags are permanently deactivated by a deactivation command, or by burning a fusible link. Sometimes the "PAID" sticker placed directly on top of the EAS tag is a blocker, so the tag underneath is never really deactivated. Tags may be temporarily deactivated with sleep and wake commands [17], thus allowing beneficial home uses after the reversible deactivation during store checkout. Tags can be permanently deactivated by a kill command, electrical attack (microwaving or strong EMP), or physical attack (pulling off the antenna or just pulling a tab that severs the antenna connection). RFID equipped U.S. Passports allows access control with shielding in the covers so it can be read only when opened and the data is encrypted using a key that's inside the passport [18]. Temporary deactivation is achieved in many ways, such as using a shielded bag or wallet to block detection or access of any RFID devices inside. Even EZ Pass can be selectively blocked with aftermarket shielded holders. RSA blocker tags interferes with the reader's ability to read any other tag in range by replying to all possible ids, or a range of ids for selective jamming [19], [20]. The RFID Guardian [21], [22] is more than just an RFID jammer, it is a location aware multifunction device that logs all RFID activity and selectively allows access either by allowing the reader to read the tags directly, or by acting as a proxy by emulating a tag's response. Location aware means the RFID Guardian behaves differently depending on the situation: at home it may

allow all access but away from the home it may block all access unless explicitly permitted. Eventually it will be the size of a PDA or perhaps embedded into a cellular telephone so it will be portable and convenient to use.

RFID access control such as selective blocking relates to medical compliance because it is desirable for the medicine's RFID tags to remain active for beneficial tracking but deny access outside of those boundaries. Such devices empower the patient to set their own privacy policies.

3.4 RFID Security

Just as there is a wide variety of RFID device capabilities (from sending only a pre-programmed ID to battery powered microprocessors capable of cryptographic challenge-and-response) and sizes (from grain of rice to cigarette pack size), there is a variety of security options. The limited radio range of the tag's transmitter is an advantage for that limits the range a receiver may receive useful information. Most tags offer no encryption because it is not warranted for the application. As the data is more precious, then more measures to protect the data are warranted. When analyzing and evaluating security systems [23], one must consider

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

When analyzing the privacy of medicines, there are several perspectives. The "end user" patient can benefit from machine-readable containers because that allows home devices to track the medication and assist them with following the prescription. Since the data can be read from a distance without any consent, there are concerns that criminals may scan people for high-value medicines to steal, or merely spy on them to ascertain their medical conditions, thus all the recent concerns and literature concerning tag blocking and deactivation. The primary motivator at this time is the pharmaceutical industry itself for thwarting counterfeiting and assisting pharmacists and hospitals assure only the proper medications are dispensed.

If one can see the pill bottle or read the label, then shielding the RFID is of little value: the pill type and quantity is already ascertained. Encrypting sensor network transmissions is of little value because the presence of the transmission indicates activity. Such sanity checks show when such security is not warranted. Cost per tag is a major obstacle to manufacturers, but is easier to justify for re-useable containers.

Eavesdropping on radio communications is now possible using readily available commodity parts. A RFID skimmer [24] can read tags from a distance of approximately 25 cm (50 cm is theoretically possible). The large antenna is easily hidden in a backpack or a briefcase so it could easily get within range of people in crowded situations such as an elevator, or merely sitting near the victim for a few seconds. This has been successfully demonstrated for cloning a Mobil Speedpass now that the encryption has been compromised [25].

Wardriving (traveling around with RFID detectors to locate readers, or portable readers to locate RFID tags) has expanded from the WiFi arena to RFID [26], [27].

Malicious RFID tags could attack readers by overwhelming the reader with data (for a denial-of-service attack), or by presenting malicious data (commonly called phishing) [28] although some doubt its effectiveness due to filtering and scrutiny of RFID input [29].

Switching price tags on store items is an old and simple method of giving yourself a discount, assuming an inattentive cashier does not notice the discrepancy. Web sites such as www.re-code.com demonstrate how to accomplish that by switching barcodes with those of similar items, again assuming an inattentive cashier. That is why self-scan checkouts have a camera over the scanner: for a human to correlate the item scanned to the price and description. As an act of further defiance, items on the shelves may be re-labeled or altered for others to unknowingly take the benefit or blame. If reprogrammable RFID tags are deployed in stores for individual items then it is reasonable to speculate that similar attacks are possible by deactivating the tags, erasing them or reprogramming with the valid EPC for other items [30]. Overconfidence in RFID checkouts will only facilitate such success since items are not scrutinized for matching price or description. That may lead to an escalation of store surveillance to include electronic-warfare type countermeasures such as detectors for RFID programmer activity in inappropriate areas or at inappropriate times.

A countermeasure to such attacks is by using protocols that only accept input from authenticated sources. Unfortunately, some attacks use these protective measures as an attack. For example, most blocker tags jam just a portion of a transmission so the CRC fails and the entire transmission is discarded. Here is a quick overview of the evolution of error detection pertaining to data communications.

Table 3.1 Data Assurance Methods

method	lifetime	security
parity, checksum, crc, ecc	forever	none
hash	forever	medium
mac	duration of shared secret	high
electronic signature	until key is revoked	high

When data communications or storage systems talk of data assurance, the emphasis is on error detection and correction. ROMs use a checksum to guard against data corruption because bits tend to fail in the same way. Transmission errors are often bursts, thus the need for a CRC to catch many bit changes that may occur in either direction. Hard drives & RAM uses ECC for detecting errors with greater confidence, and recovery from many errors, trading off memory capacity for reliability

A hash (such as SHA-1 or MD5) is a one way (or trapdoor) function where it is difficult to predict the outcome for given input. A good hash is similar to a good encryption system: the output should be as close to random as possible and it should exhibit an "avalanche effect" (small changes in input result in large changes in output). The reason for the added complexity is to thwart intentional data manipulation. When software or important files are transmitted, their hash is often sent via another channel to affirm that the files are genuine and unaltered. The "goodness" of a hash is the inability to find another input that yields the same output. Since the output (128 bits for MD5, 160 bits for SHA-1) is so much smaller than the input, it is possible for several inputs to generate the same output. That is called a "collision". Cryptographic attacks search to find inputs that create collisions but most start with carefully crafted input, not arbitrary text, so the system is still very effective for the near future.

A hash by itself does not prove the identity of the sender nor restrict reception to intended recipients but it is the building block for further data assurance.

A MAC (Message Authentication Code) builds upon the hash by mathematically combining the hash with a secret key that the sender and recipient have pre-determined, thus proving that the message was unaltered and originated from one of the key-bearers. The problem with a MAC is that it is only useful while the shared secret is still secret, and it does not prove who originated the message since all participants have the same information. Any compromise of the shared secret allows an imposter to create valid MACs for their messages and thus may impersonate a member of the secure communications session. Since safeguarding the shared secret is a problem, MACs are best used only during a communication session and changed during long sessions.

A digital signature combines hashes with Public Key (asymmetric) cryptography by combining the hash result with the originator's private key to create the digital signature (an operation only the sender can perform because the private key is required). Any recipient can verify the signature by submitting the message, signature and originator's public key to a verification "box" (usually a software module) which returns a yes or no answer. This protects the data from alteration over a long time and may be stored in a database to authenticate the origin of the data. Digitally signed data may optionally be transmitted via an encrypted channel to provide further mutual authentication, thus preventing eavesdropping or other transmitters from inserting or replaying data. The value of a digital signature over encryption is that the data is NOT encrypted: it is readily available. The signature does not interfere with access to the data, it provides a way to prove that it is unaltered and the origin. Any device that generates

data can benefit from applying a digital signature to results that are transmitted so the record cannot be altered or repudiated.

This relates to RFID because the data stored on an RFID tag describing a drug's origin may be electronically signed, thus preventing alteration and proving the origin of the message. But the message and signature can be cloned and replayed unless further precautions are used in every hop the message takes. Encrypting a channel is useless if an intruder alters the database via another point of ingress. All these precautions must be used together to assure no "white spots" (places where data is insufficiently protected).

Most digital communications offer parity or CRC to assure error-free data reception, but that is insufficient to guard against malicious data alteration or insertion, thus the need to understand and use other data safeguards in addition. If, however, the lower link layers use encryption that provides authentication (such as IPSec), then there is no need to duplicate that effort.

3.5 RFID With Sensors

While most RFID tags are totally self contained, some have sensors so they may transmit their status. Sensor networks and RFID overlap for they both provide ways to wirelessly measure things. Batteryless RFID tags may measure things if the sensor operates without power. Smart Pebbles™ [31] – [33] uses chloride sensors in small RFID tags that are buried in roads and bridges to detect impending corrosion. SensorTags™ place thin heat sensors between the space shuttle tiles for measuring if a threshold temperature was reached during the mission. There has been speculation about placing RFID sensors

inside meat packages to assure freshness, on refrigerated packages to warn if it was ever improperly stored, but at this time such sensors are too expensive for mass deployment.

3.6 ZigBee and Other Sensor Networks

AutoID is the new name for machine-readable technologies – not just a list of specific implementations, technologies or standards. Many devices that can call themselves RFID are not limited to just the commonly implemented frequencies & protocols (in fact, many were proprietary before the standards caught up). Some RFID devices have battery powered microcontrollers and active sensors, thus overlapping with sensor-networks, motes, mobile networks and other data-gathering network devices. ZigBee is a new network protocol, similar to Bluetooth, but focused on sensor networks where slower data speed is acceptable, long battery life is essential (since many may be inaccessible once deployed). A full ZigBee protocol implementation allows for large networks (thousands of nodes) in various topologies (mesh, cellular), with authentication and encryption. ZigBee is positioned to be a major wireless technology in the near future, competing or overlapping with RFID for many applications.

CHAPTER 4

DESIGN

4.1 Multiple Pill Detection Modes

Several different modes and sensors are demonstrated to compare reliability, failure modes and cost.

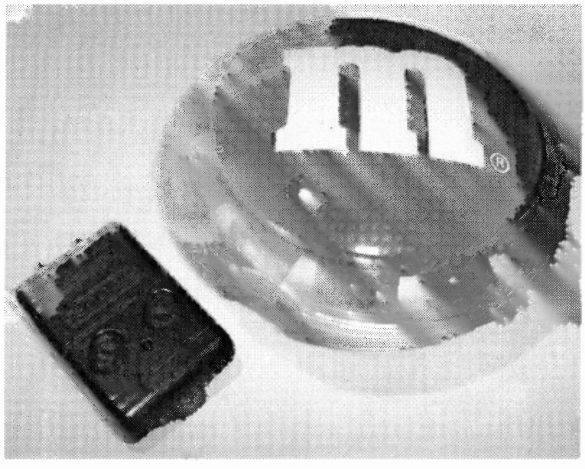


Figure 4.1 Candy dispenser prototype.

This prototype uses a motorized candy dispenser attached to a fob-style transmitter. Operating the dispenser to release a pill also activates the transmitter. The number of pills dispensed can be inferred by the transmission length if the button is held down. A receiver must within range and connected to a recording device such as a computer which is responsible for notifying a caregiver if no pills are taken for a pre-determined interval. The receiver may monitor several such containers.

Advantages of this method:

- Uses a small COTS (Commercial off-the-shelf) transmitter such as an RKE (Remote Keyless Entry), modified wireless mouse, keyboard or game controller.

Early RKEs used a simple encoding scheme with a pre-set ID, thus allowing cloning. More recent models use rolling codes to prevent cloning, therefore providing authentication.

- monitoring cannot be circumvented
- pill removal is reported in real time
- novelty of the dispenser may appeal to children

Disadvantages of this method:

- must preload the dispenser with pills
- not all pills may fit the dispenser
- base station must always be on to receive notifications
- status is not recorded if the dispenser is out of radio range

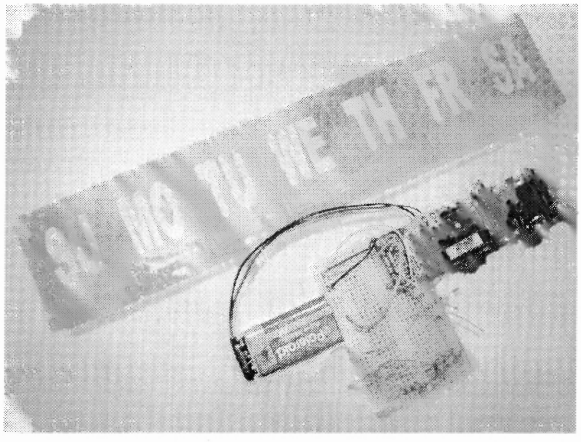


Figure 4.2 Pill box prototype and controller.

The second prototype is a multi-compartment pill container where pills are sensed by

- A sensitive switch underneath the pill compartment
- A reflective photosensor on the side of the pill compartment
- A LED shining across the pill compartment to a phototransistor (A "U" shaped plastic is inserted into the compartment to assure that pills block the beam).

The controller's RS232 serial port is connected to a variety of devices, such as a cellular phone (for sending SMS text messages) or a wireless modem to a central node (usually a Personal Computer with internet connection for sending status via email or email gateway to fax or cellular phone next message).

Advantages of this method:

- Works for any number of pills per chamber
- Easier to fill the container
- Stand-alone configuration is possible using a cellular phone

4.2 Why ZigBee

ZigBee is a new wireless standard that is similar to Bluetooth (both are PAN: Personal Area Networks with range up to 10 meters) but it is designed specifically for sensor networks, featuring long battery life, secure communications, scalability (to thousands of nodes) and many modes of collaboration among the nodes. The development hardware and software are often free or highly discounted as venders promote the new standard. The prototype was build using a developer's kit of hardware and software that was free from the Freescale sponsored contest [34]. The production hardware will be inexpensive

(even without subsidies) once mass produced. The short range is appropriate for this application because it's being used as a "near contact". Unlike most RFID tags that are totally self-contained (no external inputs), ZigBee is intended for integration into embedded systems, thus the natural ability to add active or passive sensors. ZigBee can be considered an "active" or self powered RFID tag. Requiring batteries is usually considered a drawback, but it is also advantageous for that allows for an "off switch" and user control of the device, similar to the original Active Badge design.

Table 4.1 ZigBee Key Features

- Ratified as IEEE standard 802.15.4, thus assuring compatibility among suppliers
- Has the potential to last as long as the shelf life of most batteries
- Multiple levels of security ensure that the network and data remain intact and secure.
- CCA (Clear Channel Assessment) provides a mechanism for ZigBee networks to look for and avoid other wireless networks, such as Wi-Fi
- Message acknowledgement helps to ensure that the data was delivered to its destination
- Supports Star, Mesh and Cluster Tree networks. Mesh networking can extend the range of the network through routing, while self healing increases the reliability of the network by re-routing a message in case of a node failure
- Supports 3 different frequency bands, providing customers the flexibility to choose what band best suites their needs.

Source: www.freescale.com/zigbee.

CHAPTER 5

IMPLEMENTATION AND RESULTS

5.1 Prototype #1: Modified Candy Dispenser

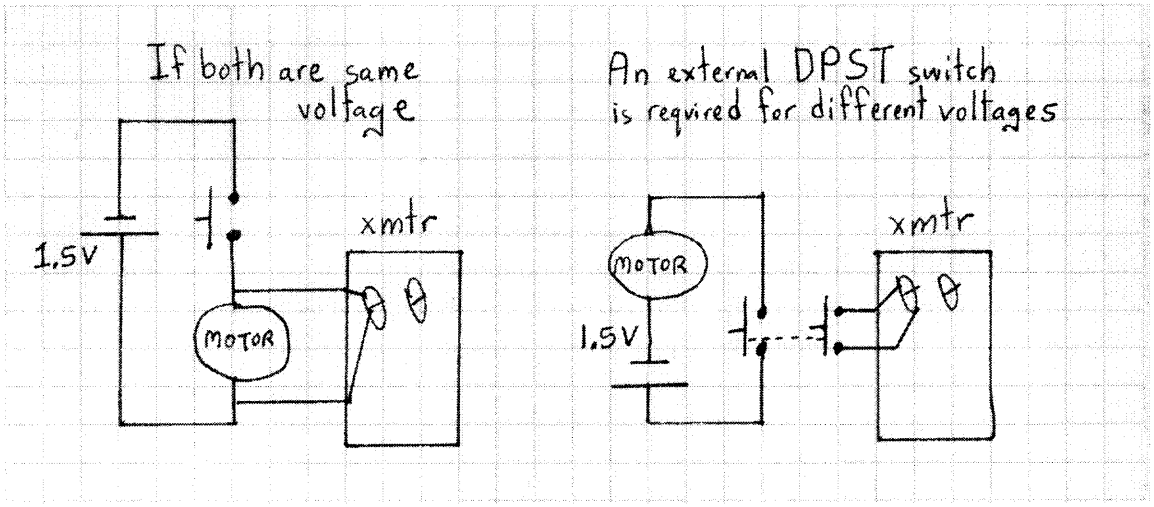


Figure 5.1 Schematic of candy dispenser.

The candy dispenser prototype may be as simpler as 2 wires if the candy dispenser and wireless device operate at the same voltage. If the devices are different voltages then an external double-pole single-throw normally-open switch is required for isolation. The receiver is attached to a Linux PC running a program that logs incoming events (see Appendix A.2-4 for the program listings). Every day (or more often if desired) CRON (the clock daemon) runs a notification program on a recurring schedule to e-mail the caregiver if no activity occurred. The email may be directly to the caregiver's email address, or relayed to a cellular phone as a SMS (text message) if the carrier provides an email gateway. The actual messages are programmable. The example sends the message "Jeff missed his daily medication, please check up!" to my cellular phone if no activity is recorded since the last time the notification program was executed.

5.2 Prototype #2: Multimodal Pill Container

A multi-partition pill container was modified with several sensors to detect if all the pills have been removed from any chamber. The following methods are used

- Weight via sensitive microswitch
- "electric eye" sensor through the chamber (LED and phototransistor)
- Reflective optical sensor module (detecting range 5-15 mm)

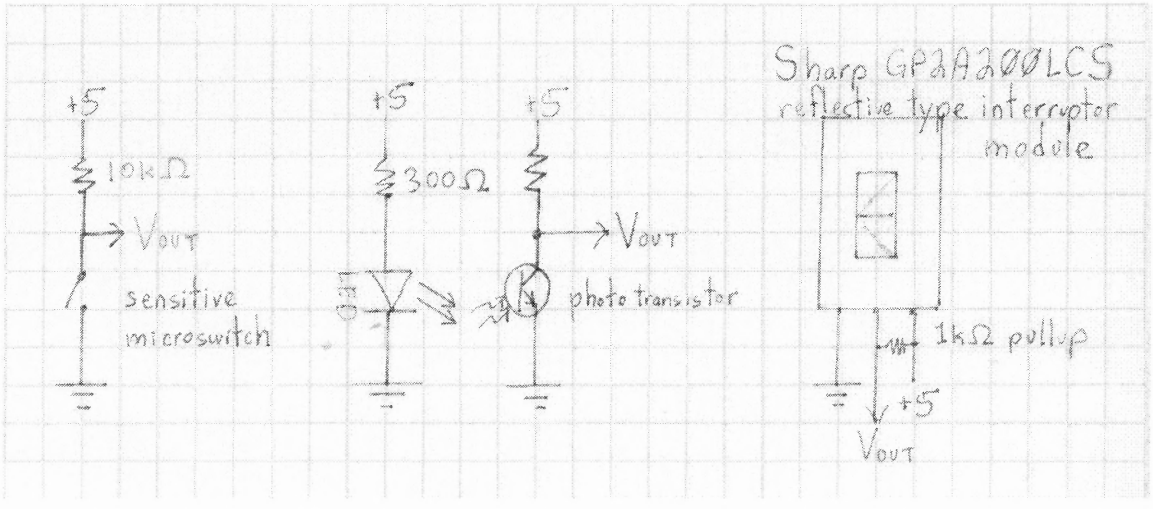


Figure 5.2 Schematic of pill container sensors.

The sensors are read by a PIC-18 microcontroller by polling all inputs every second (see Appendix A.1 for the embedded "C" program, appendix B for the PIC kit schematics and pinouts). A 9 volt battery connects to PIC module and supplies +5V to the sensors. A cellular phone, ZigBee module or other communications device attaches to the DB9S RS232 serial port.

Table 5.1 PIC Processor Connections		
18f252 pin	**Module connector**	**I/O**
	1	Ground
2	10	Analog input from reflective sensor
3	9	Analog input from phototransistor
12	3	Digital input from pill sense switch
13	2	Digital input: mode select (verbose / SMS)
14	-	Onboard LED
	11	+5 V out
	Power	9 volt battery
	DB9S	RS232C serial interface

The switch input is classified as "pills present" or "compartment empty" and the analog inputs are digitized and classified as "pill present" or "compartment empty" by pre-defined hi and low values that form a hysteresis to prevent ambiguous readings. Only changes since the last polling are reported. A switch on input RC2 (CPU pin 13) selects the message format appropriate for the device attached to the RS232 serial port. The LED on port RC3 blinks to indicate when the inputs are polled.

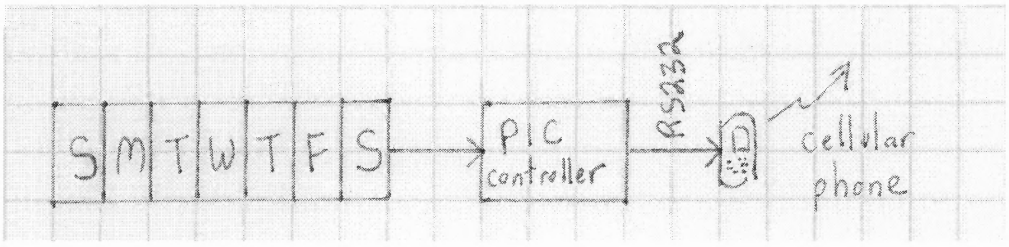


Figure 5.3 Pill container stand-alone configuration.

Attaching a cellular phone to the serial port allows independent operation, sending text messages when pills are removed or replenished. Authentication and time-stamping the event is delegated to the cellular phone system (most phones record the time a text message is received).

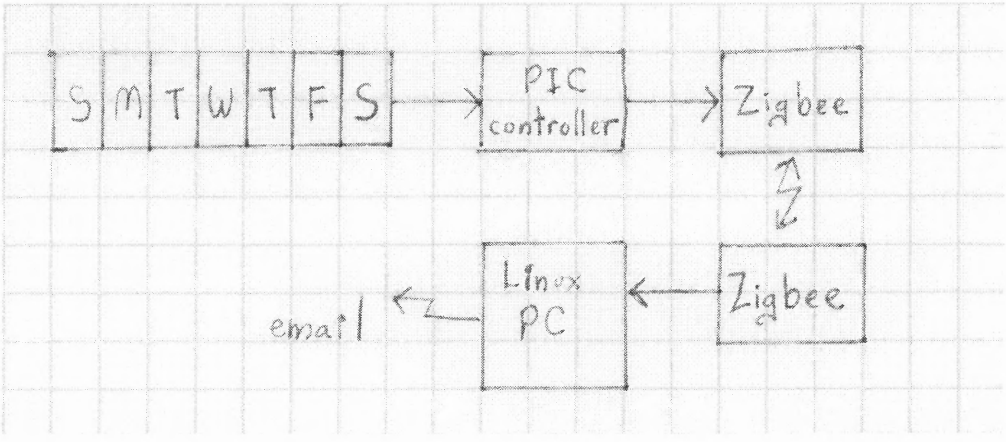


Figure 5.4 Pill container PAN configuration.

Attaching a wireless communications device such as a ZigBee module communicates to a base station for event logging, analysis, retention and notification. For the prototype, a Linux PC is used with the same software as the candy dispenser for logging events and sending daily status via email (see Appendix A.2-4 for program listings)

CHAPTER 6

CONCLUSIONS

The modular mix-and-match approach has demonstrated that affordable building blocks can give useful information, either by working stand-alone or participating in a larger monitoring system. The cellular phone configuration is of particular interest to people who want to help a loved one with a moderate budget.

The prototypes are very rudimentary and lack the robustness and features required to make them actual products. The next chapter discusses required enhancements, particularly security and privacy aspects that must be considered before deploying any such device.

There are many technical issues concerning telemedicine particularly because so many systems are highly integrated. Interdisciplinary approaches are required to balance privacy with speed and ease of use. So much research, interest and literature has recently been produced that most of the research focused on those aspects, particularly since most literature was very narrow in scope. The value added of this thesis is the correlation of new developments regarding technologies and difficulties in the telemedicine arena.

CHAPTER 7

FUTURE WORK

7.1 Prototype Enhancements

The candy-type dispenser would benefit from these enhancements:

- Removable tray for cleaning & easy loading.
- Trays with different sized compartments for different sized pills, caplets, etc. .
- Positional sensor to detect how many pills were dispensed, allowing delayed status for times when notification was not received (such as being out of range).
- Use a wireless device such a garage door opener or Remote Keyless Entry system with strong encryption (such as Microchip's KeeLoq [35] or Atmel's RKE [36]) to provide authentication and prevent spoofing or replay attacks.

The multi-chamber pillbox would benefit from these enhancements concerning pill detection:

- Try other positions of the photosensors to detect pills (such as on the bottom of the compartment), perhaps using multiple sensors per compartment.
- Use missing pulse detection to prevent ambient light interference.
- Try other sensors such as pressure, weight, capacitance to detect pill presence.
- Add tilt and motion sensors to report when it was handled (or knocked over by the cat), and to disable pill status when the box is not level.
- Use the interrupt-upon-change feature for the digital switch inputs so the CPU can use SLEEP mode to conserve battery power (currently it busy-loops and polls all inputs). Similarly, enabling interrupts for the analog inputs instead of busy-loops allows the CPU to SLEEP during peripheral activity. The prototype does not use interrupts because such code is significantly harder to write and debug.

When used with a cellular phone:

- Read the notification phone number from the cell phone's address book (the phone number was hard-coded in the prototype), thus eliminating any user-interface (number setting and modification is then a function of the cellular phone, not the pill monitor). That preserves the "baby-monitor" model that it's an appliance with only an on/off switch.

- Allow multiple numbers for notifying several caregivers

- Add a real time clock for timestamping events, and to allow daily notification instead of only real-time notification when pills are removed or refilled. The downside of this is requiring some method of setting the clock and assuring its accuracy since the device should not have any user interface (although a clock display may be considered useful).

- Expand the SMS (text messaging) command processing to a chat script similar to those used to dial modems in HoneyDanBer UUCP. This requires many changes such as converting all I/O from polling to interrupt-driven with a receive buffer, checking the responses for strings instead of a single character, error handling for when the expected reply does not arrive, adding a watchdog timer to prevent blocking when replies don't arrive, adding a-priori knowledge to handle different command sets from various cellular phone manufacturers and models.

When connected to a PC via cable or wireless link:

- Use a secure communications protocol including digital signature and mutual authentication to assure privacy and integrity of the data collected (the ZigBee protocol has such provisions, but they were not enabled for the prototype). New technologies such as Handshake Solutions' totally asynchronous CPUs may reduce the power requirements sufficiently so strong encryption is within the power budget.

- If events are not logged in real time then a real time clock is required to timestamp the events for later retrieval. Unlike the cellular phone scenario, it is reasonable to assume a bi-directional protocol, so the PC could also set the time to assure time synchronization of all data sensors.

- Concealed buttons for the user to selectively permit restricted activities such as resetting the ID or firmware upgrades.

A current attack on reprogrammable devices (wireless or not) is to reprogram the parameters or insert malicious code. Factory default passwords are an insufficient deterrence because most devices are never properly administered. Attacks on wireless networks and devices are already being practiced. Even cellular phones are now vulnerable to receiving malware. To protect the wireless devices from attack yet allow upgrades, there must be a way for the user to grant permission for the protected action. A simple method to indicate that consent is to push a hard-to-press button such as using a paper-clip to press a button behind a hole, or pressing a recessed button (similar to the buttons used to set clocks and watches).

7.2 Better Sensors

The ideal sensor is one that requires no power to sense that the bottle was opened, holds its state until read and is electrically reset. A bistable MEMS switch would be ideal if it could be latched externally (perhaps by a magnet similar to a reed switch), but reset electrically after its position/status was read (unlike a hall-effect sensor which requires power to operate and has no memory-effect). This would sense when a container cap is opened, thus implying medication removal. A small magnet located on the container latches the bistable MEMS switch inside the cap during container opening or closure. The switch is wired to an RFID chip with input pins such as the Microchip MCRF202 [37] to transmit the status and harnesses power from the reader to reset the switch for the next event.

Magneto-restrictive devices may be useful as sensors for they retain their state without power, their properties can be altered externally by a magnet, and reset

electrically. Muscle or memory-metals may be used as switches if opening the container deforms the metal in a detectable way and it can be reliably reset by the reader either electrically or by heat. Piezoelectric cells may be useful not only for sensing container activity but also to generate electricity to power other sensors and the microprocessor long enough to record the activity for reading later.

Active sensors near the medicine may gather additional information to further qualify activity. E-field sensors are non-contact people sensors, which may be useful for activity monitoring and for knowing if the patient was near the medicine or even handled it without taking any dosages. RFID readers may be useful in multi-person households to correlate medicine removal with the RFID-tagged person in close proximity.

7.3 Aftermarket Containers

When an RFID reader is added, there are tradeoffs concerning the sensor and antenna positions on the container.

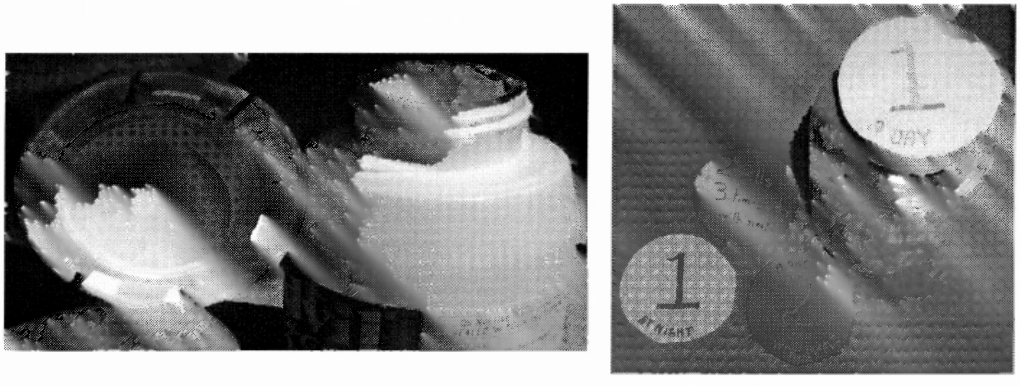


Figure 7.1 Easy grip caps.

Many caps are large so they are easy to grip, or have child-resistant mechanisms. There is ample space inside such caps for sensors to detect the container being opened,

the electronics and antenna. Such caps could be made to fit existing containers so there is no need to transfer the medication, and the original prescription label stays on the container. These caps could also have large easy to read labels for directions. The drawback to depending solely on the caps is coping with lost or misplaced caps, or caps on the wrong bottles.

Placing the sensor and electronics in the label is best done at the pharmacy since that is where the per-patient label originates, and it assures none of the original directions are obstructed. This requires total collaboration from manufacturer to distributor to pharmacy to patient. That is not feasible at this time, but once implemented it will be the most cost effective method due to the scale of economy, particularly if it is implemented as an extension of tamper-detection. RFID in the label has greater space for the antenna but resettable sensors may be hard to attach or adhere to the label unless embedded into the container.

Embedding the RFID and sensor in the body of the container itself is probably the most expensive because it may interfere with the manufacturing process, but it allows the antenna or single-contact on the bottom for close coupling the reader (particularly useful for "smart shelves") and sturdier sensor placement.

7.4 Cryptographic Attacks

A problem with any small embedded device is that it is vulnerable to attack. It can be physically attacked or influenced to fail in ways that reveal internal status (exposure to x-rays or strong EMP, altering the power supply, asserting strong signals). Accessing the chip is usually thwarted by bonding the chip to the container or label in ways that causes

the chip's destruction if access is attempted, but reverse engineering has countermeasures with appropriate solvents and micro-saws. Cryptographic hardware has been successfully attacked with power and timing analysis [38] – [40], so the next generation of embedded cryptographic chips are resistant to such attacks to conform to RFID e-passport requirements [41], [42].

The wireless network is vulnerable in many ways such as eavesdropping and intrusion. Battery-less devices are extremely resource limited. Even with low power microprocessors and embedded cryptographic hardware, public key encryption typically requires additional power (thus the batteries in the EZ-Pass).

A security analysis balances the risks with the value of the data. As previously discussed, the home user is not the primary target of attacks, and there are many countermeasures already available. Anyone who can physically see or touch the pills can read the label and see how many are in the container, so there's little sense in taking extraordinary measures to thwart physical detection of the medicine.

Attacks on sensor networks may be tampering, jamming or link layer attacks. Some of these attacks may be inadvertent (other devices using the same frequencies, a failed sensor transmitting bad ID or data or impersonating valid devices by duplicating their IDs) [43]. Designs that include security measures such as mutual authentication and data assurance in the initial design will gain greater deployment and trust than those open to such risks.

7.5 HIPAA and Privacy Laws

Ask any medical professional about HIPAA and watch the pained expression on their face. HIPAA compliance is a current "hot topic" because it is so far-reaching and not well defined. The intention is to assure confidentiality of patient data. It is achieved via stricter control and auditing of who may access the data than ever before. Overly strict interpretations leads to situations such as emergency rooms being afraid to call patients by name for that is disclosing their identity to everyone in the room. Pharmacists are now more responsible for patient and prescription privacy. If such information is encoded on the medicine's RFID, then it could be vulnerable by snooping (intentional spying [44], or unintentional). Another danger is the longevity of the RFID tag: unless destroyed or deactivated before disposal, the tag may retain the data indefinitely and it cannot auto self-destruct because there is no battery or way to supply a trusted clock. Encrypting the data, mutual authentication or other access controls would protect against unauthorized access during the intended product lifetime and beyond.

7.6 Integration with Pharmaceutical RFID

The CVS RFID initiative is noteworthy for their HIPAA compliance. Two stores participated in the initial trial, tagging every dispensing bottle and customer vial. Since the average prescription costs $55.00, a 20 cent tag is cost effective

> With 4,087 stores and 110,000 employees in 33 states, CVS/Pharmacy Corporation fills 10.6% of all drug prescriptions in the United States.
>
> - member of MIT's Auto-ID Center
> - project Jump Start: pharmaceutical industry's first RFID trial deployment: used on only 10 drugs, a case of 72 bottles would have 73 tags [one per container and the case/box too, and]focuses on: outdates (expiration), recalls, returns, damage
>
> Q: With Jump Start you're working hard to make sure that consumers never get an RFID tag, not even a killed one. Why the concern?
>
> A: Because the privacy guidelines haven't been finalized, because there hasn't been privacy education for the consumer, and because there isn't a killable tag in our pilot, we decided to take a removable-tag approach. There will be a little flag on every vial. We are going to tell customers they can rip off the flag if they choose. We're going to notify the customer in a number of different ways. There will be signs in the store. There will be a little monograph in the bag. And there will be a label on the tag. That's for the trial. When we go into production, the RFID tag will be applied under the prescription label, and we'll use a kill command - we will kill the tag before it is placed in the customer's hands.
>
> Source: S. Garfinkel, J. DeAlmo, S. Leng, P. McAfee and J. Puddington, "RFID in the pharmacy: Q&A with CVS." in *RFID Applications, Security and Privacy,* S. Garfinkel, B. Rosenberg, Ed. Upper Saddle River, NJ: Addison Wesley, 2006, pp. 208-209.

Once RFID enabled home-monitoring systems are common, customers ought to have the choice to keep the RFID tag enabled. Mail order pharmacies ought to keep the RFID tag enabled for the recipient to verify the prescription even if not yet integrated to the medicine compliance system.

7.7 Closing The Loop

Detecting if pills were removed from the container is no guarantee that the medicine was actually ingested. If many pills are missing, was it an overdose, an accidental spill, or were some transferred to an unmonitored container?

Most prescriptions are based on statistics, not the patient's daily needs or reactions. Applying control theory to medication requires constant measuring and monitoring the body's reactions and functions, adjusting the medication dosage, noting the body's reaction and repeating. Such a system would automatically detect side effects, interactions with other medications (or substances such as alcohol, tobacco), and detect changes in health.

In some circumstances, patients may be legally required to adhere to a medication schedule. Clever patients may intentionally circumvent a simple monitoring system if they don't want to comply with their medications. That warrants stricter observation such as more frequent supervision supplemented by implanted tamper-resistant sensors to assure the medicine was administered in sufficient strength to be effective and is not rendered ineffective by other substances.

The "smart pillbox" can participate in such a system. If the bio-sensors report that no dosage is required today, then the patient is notified that no pills should be taken and ANY medicine taken from the pillbox is reported as an error. If the dosage is increased based on activity, then the number of pills the dispenser reports as removed ought to match. So even in a closed loop system, this pill sensor is useful for reporting when medicine was dispensed: how much, when, qty left. Integrating RFID would show expiry, spoilage (ex: insulin too hot) and help automate medicine compliance.

APPENDIX A

PROGRAM LISTINGS

Appendix A.1 is the embedded "C" language program programmed into the flash memory of a PIC 18f252 microcontroller. It monitors a pillbox using various sensors to detect pill removal, and either transmits plain text message for change of status, or sends the message to a cellular phone attached to the RS232 serial port using the SMS protocol. The following Linux program and configuration files monitor and report activity from either the candy dispenser or pillbox prototypes:

- Appendix A.2 is the program that receives the wireless status and logs the event into a file.
- Appendix A.3 is the cron configuration file that runs a program to notify the caregiver. Notification may be daily or more often, as desired.
- Appendix A.4 is the daily status program that notifies the caregiver via email or text message.

The Linux software can be modified to operate under Windows using Cygwin or other POSIX environments.

A.1 Source Code: Pill Sensors

```
/*
 * Source code to read pill container sensors
 * By Jeffrey S. Jonas
 *
 *    Development environment:
 *    software:
 * The Microchip C18 "C" complier and libraries
 *    hardware:
 * The APP-III GPMPU28 PIC development board by
 * AWC Electronics contains
 * - 18f252 single chip microcontroller featuring
 *    . on chip 5 channel A/D (multiplexed input)
 *    . other pins may be programmed as
 *      digital input or output
 *    . on chip UART
 *    . on chip FLASH, EEPROM and RAM
 * - 20MHz resonator
 * - RS232 level shifter and DB9S connector
 * - 5v regulator powered by a 9v battery
 * - 11 pin edge connector for interfacing to devices
 * - reset switch, one output-controlled onboard LED
 * see: http://www.awce.com/app3kit.htm
 *
 * PIN ASSIGNMENTS
 *  +-- 18f252 chip
 *  |   +-- card edge
 *  |   |
 *  2  10 AN0   : analog input 0 from pill 1
 *                reflective photosensor module
 *  3   9 AN1   : analog input 1 from pill 2 photosensor
 * 12   3 RC1   : digital input: pill 3 compartment switch
 * 13   2 RC2   : digital input: mode select
 *                (verbose / SMS)
 * 14   - RC3   : onboard LED
 * 17   - RC6/TX: uart transmit to DB9 pin 2
 *                via rs232 level shifter
 * 18   - RC7/RX: uart receive to DB9 pin 2
 *                via rs232 level shifer
 *
 *    Setting card pin 2 HIGH sets SMS_FORMAT
 * so the cellular phone on the RS232 serial port
 * sends text messages (SMS) to the
 * pre-programmed phone number.
 *    Setting card pin 2 LOW sends plain text messages
 * to the ZigBee wireless adapter (or direct connect cable)
 * on the RS232 port to a home PC to log the events
 * and send daily status via email or SMS-gateway.
 */

#include <p18f252.h>
#include <stdio.h>
#include <delays.h>
#include <usart.h>
#include <adc.h>  // analog input definitions
```

```
extern union USART USART_Status;

// external input chooses plain text or SMS messages
const int PILL1_REMOVED=0;
const int PILL1_REPLACED=1;
const int PILL2_REMOVED=2;
const int PILL2_REPLACED=3;
const int PILL3_REMOVED=4;
const int PILL3_REPLACED=5;
const int MODE_MSG = 6;

#define SMS_FORMAT PORTCbits.RC2  // input RC2 chooses SMS or verbose
output

// analog input is 10 bits, so the range is 0-1023
const int ANALOG0_HIGH = 220;  // define a hysteresis for unambiguous
readings
const int ANALOG0_LOW  = 200;
const int ANALOG1_HIGH = 220;
const int ANALOG1_LOW  = 200;

rom const char * rom const full_message []
={
    "pill removed from compartment 1\r\n",
    "compartment 1 REFILLED\r\n",
    "pill removed from compartment 2\r\n",
    "compartment 2 REFILLED\r\n",
    "pill removed from compartment 3\r\n",
    "compartment 3 REFILLED\r\n",
    "Verbose mode\r\n",
    "SMS mode\r\n"
};

// the cellular phone command to send a SMS text message
// including the length field
rom const char * rom const sms_cmd []
={
    "AT+CMGS=41\r",
    "AT+CMGS=33\r",
    "AT+CMGS=41\r",
    "AT+CMGS=33\r",
    "AT+CMGS=41\r",
    "AT+CMGS=33\r"
};

// The same messages from "full_message" in PDU compressed format
// as required by cellular phones without plain text SMS support.
rom const char * rom const sms_msg []
={
// pill removed from compartment 1
"0001000B819180551512F200001FF0349B0D9297DB6F7B990C32CBDF6DD0F8DD8687E5
F476D94D07C500\032\r",

// compartment 1 REFILLED
"0001000B819180551512F2000016E3771B1E96D3DB65371D1403498BC62493592402\0
32\r",
```

```
// pill removed from compartment 2
"0001000B819180551512F200001FF0349B0D9297DB6F7B990C32CBDF6DD0F8DD8687E5
F476D94D07C900\032\r",

// compartment 2 REFILLED
"0001000B819180551512F2000016E3771B1E96D3DB65371D2403498BC62493592402\0
32\r",

// pill removed from compartment 3
"0001000B819180551512F200001FF0349B0D9297DB6F7B990C32CBDF6DD0F8DD8687E5
F476D94D07CD00\032\r",

// compartment 3 REFILLED
"0001000B819180551512F2000016E3771B1E96D3DB65371D3403498BC62493592402\0
32\r",
};


void put_verbose_message (const int msgIndex)
{
    putrsUSART (full_message[msgIndex]);
}


// Cellular phones use a Hayes-modem "AT" command set.
// This handles one command at a time
// by transmitting the command and reading back the reply.
void do_cmd (const char * const command, const char rpy_char)
{
    // flush input buffer
    while (DataRdyUSART())
    {
      getcUSART();
    }

    if (USART_Status.FRAME_ERROR) // clear any rcv errors
    {
      // printf("Error: FRAME_ERROR\r\n");
      USART_Status.FRAME_ERROR=0;
    }

    // The serial receiver can overrun if data is received
    // when not actively polling since it's not
    // interrupt driven.
    // RCSTA (the Receive Status & Control Register)
    // is explained on pg 167 of the 18f252 data sheet.
    if (USART_Status.OVERRUN_ERROR || RCSTAbits.OERR)
    {
      // printf("error: OVERRUN_ERROR\r\n");
      USART_Status.OVERRUN_ERROR=0;
      RCSTAbits.CREN=0; // clear the overflow error
      RCSTAbits.CREN=1; // to allow further data reception
    }

    putrsUSART (command); // transmit the command string
```

```
    do // read (and discard) the reply until the terminating character
    {
      while (!DataRdyUSART()) // wait for character available
          ;
      if (USART_Status.FRAME_ERROR) // clear any rcv errors
          USART_Status.FRAME_ERROR=0;
      if (USART_Status.OVERRUN_ERROR || RCSTAbits.OERR)
      {
          USART_Status.OVERRUN_ERROR=0;
          RCSTAbits.CREN=0; // clear the overflow error
          RCSTAbits.CREN=1; // to allow further data reception
      }
    } while (getcUSART() != rpy_char);
}


// Send the command sequence for a cellular phone to send a text
message (SMS)
// given a pre-formated message in PDU compressed format.
void putSMS (const int msgIndex)
{
    do_cmd ("\rATE0\r", 'K');      // command echo OFF, wait for "OK"
    do_cmd ("AT+CMEE=1\r", 'K');  // set numeric error codes
    do_cmd ("AT+CMGF=0\r", 'K');  // set compressed PDU message format
    do_cmd (sms_cmd [msgIndex], '>');  // send SMS command, wait for
prompt
    do_cmd (sms_msg [msgIndex], '\r'); // send SMS message, wait for
completion
}

void
main (void)
{
    // int i = 0; // debug only

    int sensor0, sensor1;  // the analog inputs

    // Save the previous pill compartment states to report only changes
    // Set initial status to EMPTY
    // so all filled compartments are reported on power on.
    int pill_1_status = PILL1_REMOVED;
    int pill_2_status = PILL2_REMOVED;
    int pill_3_status = PILL3_REMOVED;

    int new_status;

    // set uart to 9600 async
    OpenUSART (
      USART_ASYNCH_MODE & USART_EIGHT_BIT & USART_TX_INT_OFF &
      USART_RX_INT_OFF & USART_BRGH_HIGH, 129);

    // open 2 analog channels
    OpenADC (ADC_FOSC_32 & ADC_RIGHT_JUST & ADC_8ANA_0REF,
       ADC_CH0 & ADC_CH1 & ADC_INT_OFF);

    TRISCbits.TRISC3 = 0; // set on-board LED port to output
```

```
while (1)
{
  Delay10KTCYx(0);
  Delay10KTCYx(0); // spin-loop delay one second

  PORTCbits.RC3 ^= 1; // toggle on-board LED

  // Read all sensor status at the same time to assure coherency
  // particularly since transmitting SMS may take several seconds.

      // Read analog channel 0 for photo sensor
  SetChanADC (ADC_CH0);
  Delay10TCYx (10);     // Delay for select channel
  ConvertADC ();        // Start conversion
  while (BusyADC());    // Wait for completion
  sensor0 = ReadADC(); // Read result

      // read analog channel 1 for photo sensor
  SetChanADC (ADC_CH1);
  Delay10TCYx (10);     // Delay for select channel
  ConvertADC ();        // Start conversion
  while (BusyADC());    // Wait for completion
  sensor1 = ReadADC(); // Read result

  #if 0 // debugging
  if (!SMS_FORMAT)
      printf ("%d (%d %d %#x) mode=%S",
      i++,
      sensor0, sensor1, PORTCbits.RC1,
      full_message[MODE_MSG + SMS_FORMAT]);
  #endif


  // examine the switch input
  if (PORTCbits.RC1)
      new_status = PILL3_REPLACED;
  else
      new_status = PILL3_REMOVED;

  if (new_status != pill_3_status)
  {
      if (SMS_FORMAT)
        putSMS (new_status);
      else
        put_verbose_message (new_status);

      pill_3_status = new_status; // save the status for next loop
  }


  // process previously read analog input 0
  if (sensor0 > ANALOG0_HIGH)  // apply hysteresis
      new_status = PILL1_REPLACED;
  else
  {
      if (sensor0 < ANALOG0_LOW)
        new_status = PILL1_REMOVED;
```

```
            else
              new_status = pill_1_status; // use previous status
        }

        if (new_status != pill_1_status)  // send message only on change
of status
        {
            if (SMS_FORMAT)
              putSMS (new_status);
            else
              put_verbose_message (new_status);

            pill_1_status = new_status; // save the status for next loop
        }

        // process previously read analog input 1
        if (sensor1 > ANALOG1_HIGH)  // apply hysteresis
            new_status = PILL2_REPLACED;
        else
        {
            if (sensor1 < ANALOG1_LOW)
              new_status = PILL2_REMOVED;
            else
              new_status = pill_2_status; // use previous status
        }

        if (new_status != pill_2_status)  // send message only on change
of status
        {
            if (SMS_FORMAT)
              putSMS (new_status);
            else
              put_verbose_message (new_status);

            pill_2_status = new_status; // save the status for next loop
        }
    }
}
```

A.2 Source Code: Wireless Status Reception

```
# log_event.sh
# this shell script is invoked every time
# the key fob transmits that pills are being taken

LOGFILE=$HOME/medicine.log
date >> $LOGFILE
```

A.3 Crontab Configuration File

```
# This is the crontab file that runs the
# notification program every day.
#
# the command
#    crontab crontab_file
# needs to be run only ONCE
# to start the recurring execution
# This file is expected to be edited as needed with
# - times for notification [the crontab schedule line]
# - email of the caregiver(s) [MAILTO variable]
# - message to be delivered   [MSG variable]

# mail the warning to Jeff's cellular phone
# via the Cingular SMS gateway
MAILTO=9085551212@mmode.com

# use /bin/sh to run commands,
# no matter what /etc/passwd says
SHELL=/bin/sh

# the key fob's activities are logged here
LOGFILE=$HOME/medicine.log
TIMESTAMP_FILE=$HOME/pill_notify_timestamp

JOB2RUN=$HOME/bin/daily_job.sh

# check medication status every day at 8:02 PM
MSG="Jeff missed his daily medication, please check up!"
2 20 * * * $JOB2RUN >> $HOME/tmp/cron_out 2>&1

# check medication status at noon and 8:00 PM
# sending different messages
# 0 12 * * * $JOB2RUN MSG='Jeff missed his NOON pill'
     >> $HOME/tmp/cron_out 2>&1
# 0 20 * * * $JOB2RUN MSG='Jeff missed his NIGHT pill'
     >> $HOME/tmp/cron_out 2>&1
```

A.4 Source Code: Daily Status

```
# daily_job.sh
# Send an email to the caregiver
# if no pills were taken since last time this was executed.
# This is invoked automatically every day as needed.

if [ ! -e $LOGFILE ]
then
     echo "logfile initialized by $0" > $LOGFILE
     exit 1
fi

# Send notification if no pill activity was logged
# since the last time this was run.

if [ $LOGFILE -ot $TIMESTAMP_FILE ]
then
     echo $MSG | mail $MAILTO
fi

# Remember when this was run
# for the next execution.

touch $TIMESTAMP_FILE
```

APPENDIX B

PIC 18F252 KIT

The Microchip PIC 18f252 microcontroller module is sold as a kit by the Al Williams Company. "APP-III" refers to the 18f252 microcontroller pre-programmed with a boot loader in memory locations 0000-01FF for loading programs into the Flash Rom via the RS232 port without any other equipment. "GPMPU28" refers to the PCB board which is sold with or without parts. It was chosen because it is a totally self contained unit with power supply, oscillator, RS232 port and edge connector for easy breadboarding. Most of the microcontroller's pins are programmable as input or output. In this application, all the card edge connections are inputs with RA0-1 programmed as analog inputs (internally multiplexed to a single 10-bit analog to digital converter).

Table B.1 GPMPU28 Connections

JP1 Pin	Signal	IC1 Pin
1	Ground	
2	RC2	13
3	RC1	12
4	RC0	11
5	RA5	7
6	RA4	6
7	RA3	5
8	RA2	4
9	RA1	3
10	RA0	2
11	+5 V	

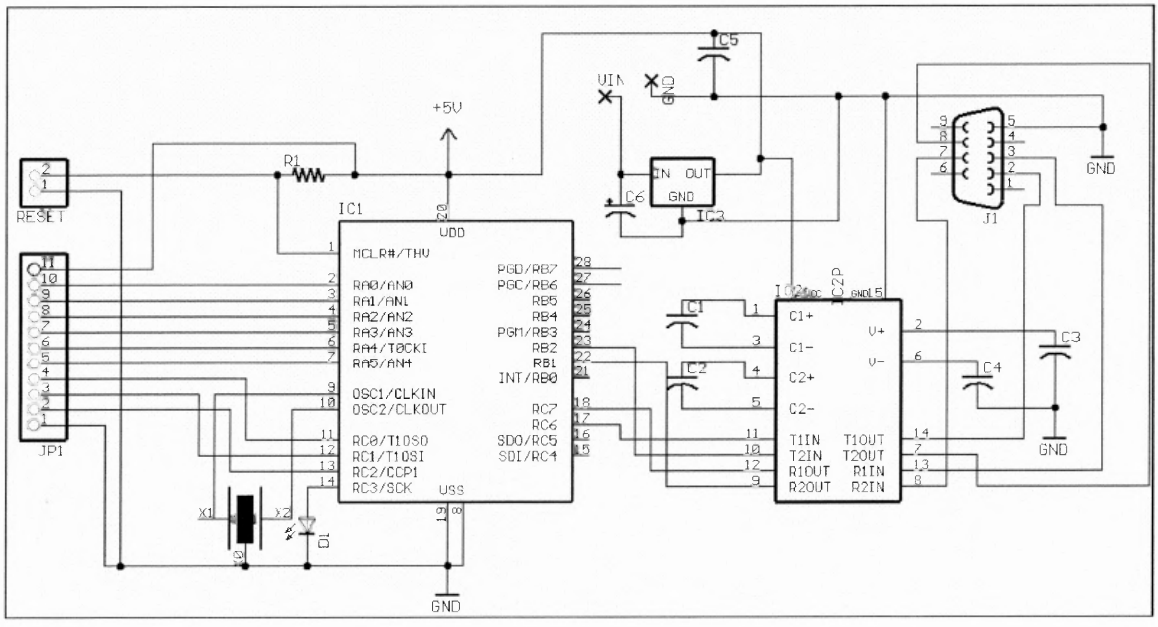


Figure B.1 GPMPU28 schematic.

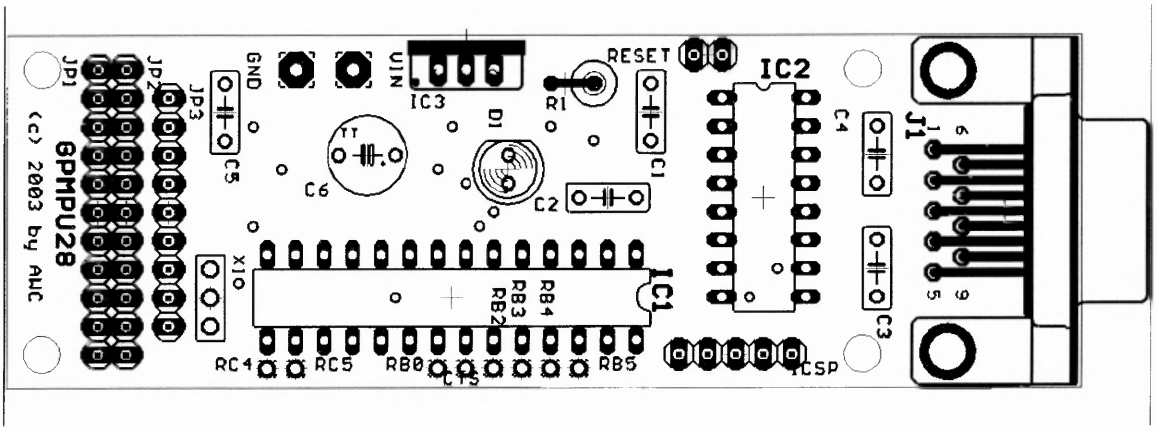


Figure B.2 GPMPU28 board layout.

APPENDIX C

IEEE STANDARDS FOR PANS

Table C.1 IEEE Wireless Standards

Standards Committee	**IEEE 802:** LAN/MAN Standards Committee			
Working Group	**IEEE 802.11:** WLAN Working Group	**IEEE 802.15:** WPAN Working Group		
Task Group	**802.11a/b/g**	**802.15.1:** WPAN/Bluetooth	**802.15.3a:** WPAN High Rate/UWB	**802.15.4:** WPAN Low Rate/Zigbee
Promoter / Industry Alliance	**Wi-Fi:** Cisco, 3Com, Agere, Intersil, Compaq, Dell, Sony, Nokia, Symbol, etc.	**Bluetooth SIG:** Ericsson, 3Com, IBM, Intel, Motorola, Nokia, Agere, Toshiba, etc.	**Wi-Media:** Appairent, HP, Motorola, Philips, Samsung, Sharp, XtremeSpectrum	**Zigbee Alliance:** Honeywell, Invensys, Mitsubishi, Motorola, Philips, etc.

REFERENCES

[1] Diabetes Mall, "Diabetes Technology: Insulin Pumps", http://www.diabetesnet.com/diabetes_technology/insulinpumps.php.

[2] Medtronic MiniMed Inc, "MiniMed Paradigm® REAL-Time Insulin Pump and Continuous Glucose Monitoring System," http://www.minimed.com/.

[3] AARP, "Magic Medicine Cabinet Monitors Meds," 2005, http://www.aarp.org/international/agingadvances/innovations/Articles/3_06_usa_accenture.html.

[4] D. Wan, "Magic Medicine Cabinet: A Situated Portal for Consumer Healthcare" in *Proceedings of First International Symposium on Handheld and Ubiquitous Computing (HUC '99),* September 1999, http://citeseer.ist.psu.edu/wan99magic.html.

[5] K. Fishkin, M. Wang, and G. Borriello, "A Flexible, Low-Overhead Ubiquitous System for Medication Monitoring," Intel Research Seattle Technical Memo IRS-TR-03-011, Oct 25, 2003, https://leitl.org/docs/intel/IR-TR-2003-134-103020031241_173.pdf.

[6] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The active badge location system," *ACM Transactions on Information Systems*, vol. 10, pp. 91--102, Jan. 1992.

[7] U.S. Food and Drug Administration, "Telemedicine Related Activities," http://www.fda.gov/cdrh/telemed.html.

[8] Project Lifesaver International, http://www.projectlifesaver.org/site/.

[9] Sheriff Froehlich's Project Lifesaver Program, http://www.ucnj.org/healthy/.

[10] K. Fishkin, United States Federal Trade Commission, "RFID Applications and Implications for Consumers", June 21, 2004, www.ftc.gov/bcp/workshops/rfid/transcript.pdf, pp.79.

[11] K. Fishkin and J. Lundell "RFID in Healthcare," in *RFID Applications, Security, and Privacy*, S. Garfinkel and B. Rosenberg Ed. New Jersey: Pearson Education, 2006, pp. 211-228.

[12] Epill.com, "Monitored Automatic Pill Dispenser MD.2 with Voice Alarm from e-pill Medication Reminders," http://www.epill.com/md2.html.

[13] K. Fishkin, United States Federal Trade Commission, "RFID Applications and Implications for Consumers", June 21, 2004, www.ftc.gov/bcp/workshops/rfid/transcript.pdf, pp. 75-82.

[14] K. Fishkin, "Ken Fishkin's Publications," Intel Research Laboratory at Seattle, 2005, http://seattleweb.intel-research.net/people/fishkin/pubs.html.

[15] EPCglobal web site, http://www.epcglobalinc.org/.

[16] Electronic Privacy Information Center, "Radio Frequency Identification (RFID) Systems," http://www.epic.org/privacy/rfid/.

[17] C. Soghoian, "RFID Security and Privacy," SPAR lab presentation, Feb 11, 2003, http://spar.isi.jhu.edu/~chris/presentations/RFID-SPAR.pdf.

[18] B. Schneier, "Schneier on Security: RFID Passport Security Revisited," August 9, 2005,http://www.schneier.com/blog/archives/2005/08/rfid_passport_s_1.html.

[19] RSA Security, "RSA Security demonstrates new RFID privacy technology: The RSA Blocker Tag," February 25, 2004, http://www.rsasecurity.com/press_release.asp?doc_id=4310&id=2682.

[20] "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," in *8th ACM Conference on Computer and Communications Security*, V. Atluri, Ed. ACM Press, 2003, pp. 103-111.

[21] RFID Guardian Project, Department of Computer Science, Vrije Universiteit, Amsterdam, The Netherlands, http://www.rfidguardian.org/.

[22] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management," Department of Computer Science, Vrije Universiteit, Amsterdam, The Netherlands, www.cs.vu.nl/~melanie/rfid_guardian/papers/acisp.05.pdf.

[23] B. Schneier, *Beyond Fear*. New York: Copernicus Books, 2003, pp. 14-15.

[24] Kirschenbaum, A. Wool, "How to build a low-cost, extended-range RFID skimmer," to appear in *15th USENIX Security Symposium*, Vancouver, Canada, August 2006, http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html.

[25] S. Bono, M. Green, A.Stubblefield, A. Rubin, A. Juels, and M. Szydlo, Johns Hopkins University and RSA Laboratories, "Analysis of the Texas Instruments DST RFID," http://rfidanalysis.org/.

[26] C. Hurle, M. Pucho, R. Rogers, and F. Thornton, *WarDriving: Drive, Detect, Defend A Guide to Wireless Security*, Syngress, March 2004, pp. 1-10.

[27] F. Thornton, B. Haines, A. Das, H. Bhargava, A. Campbell, and J. Kleinschmidt, *RFID Security*, Syngress Publishing, 2006, pp 157-162.

[28] M. Rieback, P. Simpson, B. Crispo, and A. Tanenbaum, "RFID viruses and worms," the Department of Computer Science of Vrije Universiteit Amsterdam, http://www.rfidvirus.org/index.html.

[29] Thomson, "Experts unconcerned by RFID virus," March 15, 2006, http://www.itweek.co.uk/vnunet/news/2152020/experts-unconcerned-rfid-virus.

[30] M. Rieback, "ubisec: Security in ubiquitious computing: what the hack: fun and mayhem with RFID," July 31, 2005, http://wiki.whatthehack.org/images/0/01/Fun_and_Mayhem_with_RFID.pdf.

[31] Wireless Micro-Sensors Monitor Structural Health SRI International http://www.sri.com/rd/microsensors.pdf.

[32] D. Watters, "Wireless Sensors Will Monitor Bridge Decks," http://www.betterroads.com/articles/feb03b.htm.

[33] D. Watters, P. Jayaweera, A. Bahr, D. Huestis, "Design and Performance of Wireless Sensors for Structural Health Monitoring," SRI International, http://www.dot.ca.gov/research/maintenance/docs/qnde.pdf.

[34] Freescale Wireless Design Challenge, 2004, http://www.jandspromotions.com/wirelesschallenge/index.html.

[35] Microchip KEELOQ Authentication Products, data sheet, 2006, http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=2074.

[36] Transparent receiver IC 433 MHz for RKE/TPMS, data sheet, 2006, http://www.atmel.com/dyn/products/product_card.asp?part_id=3961.

[37] Microchip MCRF202, data sheet, 2005, http://ww1.microchip.com/downloads/en/DeviceDoc/21308F.pdf.

[38] S. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-Analysis Attack on an ASIC AES Implementation," in *Embedded Cryptographic Hardware*, N. Nedjah, L. Mourelle, Ed. New York: Nova Science Publishers, 2005, pp. 51-66.

[39] K. Okeya, T. Takagi, and C. Vuillaume, "On The Importance of Protecting delta in SFLASH Against Side Channel Attacks," in *Embedded Cryptographic Hardware*, N. Nedjah, L. Mourelle, Ed. New York: Nova Science Publishers, 2005, pp. 67-82.

[40] Yu, and D. Bree, "Resistance Against Power and Timing Attacks: An Evaluation of Two Clock-less Implementations of the AES" in *Embedded Cryptographic Hardware*, N. Nedjah, L. Mourelle, Ed. New York: Nova Science Publishers, 2005, pp. 83-97.

[41] Atmel AT90SC12872RCFT, press release, 2006, http://www.atmel.com/dyn/corporate/view_detail.asp?ref=&FileName=EpassportsecureMCU_7_5.html&SEC_NAME=Product.

[42] Atmel AT90SC12872RCFT, data sheet, 2006, http://www.atmel.com/dyn/products/product_card.asp?part_id=3730.

[43] F. Anjum and S. Sarkar, "Security in sensor networks," in *Mobile, Wireless and Sensor Networks*, R. Shorey, et al., Ed. New Jersey: IEEE Press, 2006, pp. 283-307.

[44] R. Stapleton-Gray, "Would Macy's Scan Gimbels?: Competitive Intelligence and RFID." in *RFID Applications, Security and Privacy,* S. Garfinkel, B. Rosenberg, Ed. Upper Saddle River, NJ: Addison Wesley, 2006, pp. 283-290.